

Received & Inspected

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

MAR 24 2009

EB Docket 06-36

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2008

Date filed: 2/27/09

Name of company covered by this certification: GlobalNova, Inc.

Form 499 Filer ID: 826614

Name of signatory: Fabio Fonseca

Title of signatory: Controller

I, Fabio Fonseca, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules [accompanying statement attached].

The company has not taken actions against data brokers in the past year. Last year the following steps were taken to protect CPNI.

January, 2008

[Situation]: Some of the system logs were showing part of the credit card information in clear text.

[Correction]: Cryptography was applied to all credit card information that appears on system logs.

[Situation]: Part of the credit card information was stored on the database in clear text.

[Correction]: All credit card information stored on the database is now secured using the AES 64-bit algorithm.

We've hired a specialized Oracle database administration Company to help us on identifying security gaps and to design backup routines that fully protect our customer's data.

March, 2008

[Situation]: The process for renewal of SSL certificates for our websites was manual.

[Correction]: We've set a process that automatically notifies when a certificate is about to be outdated.

[Situation]: In our platform we've several tools for job management on the database. The webpage for job management was open for any user.

[Correction]: A security patch was applied and now the webpage is accessible only for registered users.

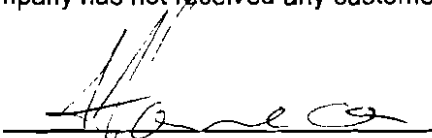
October, 2008

[Situation]: Our validation process of new passwords assigned to customers, on our website, was allowing the use of 4-digit sequences.

[Correction]: Correction in password size to improve security. The password validation process has been improved, and it now requires the use of 6-digit passwords.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed



044

Accompanying statement:

Agreements:

All non-disclosure agreements and carrier agreements must be signed by an officer of the company. GlobalNova does not allow any employee who is not CEO, CFO, Controller and Directors to sign and keep any agreements on behalf of the company. The penalty for such violation is first a verbal/oral notification and second the discontinuation of employment.

All paper agreements are kept into GlobalNova USA office locked into a cabinet file. All soft agreements (usually CDs) are kept into the same locked cabinet file. Since GlobalNova's USA office is located in the hurricane zone of Florida the company once a year sends a copy of those agreements to Brazil's office via courier.

Firewall:

GlobalNova system has a firewall configuration standards that includes a current network diagram with all connections to cardholder data. The firewall configuration standards include requirements for a firewall between any demilitarized zone (DMZ) and the internal network zone.

The firewall configuration denies all traffic from untrusted networks and hosts, except for protocols necessary for the cardholder environment.

The firewall configuration also restricts: connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks; inbound Internet traffic to internet protocol (IP) addresses within the DMZ ; prohibits the passing of internal addresses from the Internet into the DMZ; places the database in an internal network zone, segregated from the DMZ.

The firewall configuration restricts inbound and outbound traffic to that which is necessary for the cardholder data environment; denies all other inbound and outbound traffic not specifically allowed; prohibits direct public access between external networks and any system component that stores cardholder data (for example, databases, logs, trace files); controls ensure that a DMZ been implemented to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic.

IP-masquerading has also been implemented to prevent internal addresses from being translated and revealed on the Internet.

Security parameters:

All customer-supplied defaults are always changed before installing a system on the network.

All wireless environment defaults are changed before installing a wireless system.

SSID broadcasts are disabled.

WiFi protected access (WPA and WPA2) technology is enabled for encryption and authentication when WPA-capable.

Configuration standards have been developed for all system components.

The controls do ensure that all unnecessary and insecure services and protocols are disabled; ensure security parameters are configured to prevent misuse; ensure that all unnecessary functionality—such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers— have been removed.

All non-console administrative access is encrypted.

Cardholder data protection:

GlobalNova does not store the full contents of any track from the magnetic stripe nor store the personal identification number (PIN) or the encrypted PIN block.

All passwords are masked when displayed.

The passwords are rendered unreadable anywhere it is stored.

Public networks:

Strong cryptography and security protocols, such as secure sockets layer (SSL) / transport layer security (TLS) and Internet protocol security (IPSEC), are used to safeguard sensitive cardholder data during transmission over open, public networks. GlobalNova does not have any kind of wireless network with remote access to the data holder.

It is not allowed any installation of non authorized software into computers nor is permitted any access to outside web pages that are not related to the day-to-day operation of the company.

The penalty for such violation is first a verbal/oral notification and seconds the discontinuation of employment.

Anti-virus software:

Anti-virus software is deployed on all systems commonly affected by viruses (AVG for personal computers).

Customer service manual:

The customer service manual is detailed and it is basically divided into 3 parts:

I. GlobalNova. The presentation of GlobalNova and its services and products (pages 4 – 11)

II. VoIP. Definitions of most usual terms used (pages 12 – 16)

III. Call Center procedures. Details all procedures on how to deal with customers and lists all possible issues and solutions (pages 17 – 79)

The manual is written in Portuguese due to the fact that all staff and operators are based in that country. In USA GlobalNova has only two people who do clerical work. They also follow the same rules on this manual in regards to customer proprietary network information (CPNI).

All CPNI records are kept into magnetic tapes. The usage of CPNI is only allowed through a written approval from the CEO. GlobalNova doesn't print any customer's data as this is not allowed by the company rules. The only physical movement of customer's data is through magnetic tapes. GlobalNova uses magnetic tapes for database backup. Those magnetic tapes are changed weekly and moved from the data-center to our facilities within the same city. This is done through a courier service and the customer's data is cryptographed on those tapes.

GlobalNova has a process to identify newly discovered security vulnerabilities like Red Hat support which is up-to-date and also follows all the advisories.

GlobalNova has also controls to ensure: the testing of all security patches and system and software configuration changes before deployment; the removal of test data and accounts before production systems become active; the removal of custom application accounts, usernames, and passwords before applications become active or are released to customers; the review of custom code prior to release to production or customers in order to identify any potential coding vulnerability; the documentation of impact; the testing of operational functionality.

All users are identified with a unique user name before allowing them to access system components or cardholder data. In addition the password is required to authenticate all users. All passwords are encrypted during transmission and storage. All addition, deletion, and modification of user IDs, credentials, and other identifier objects are controlled by the administrative user. If a session has been idle for more than 15 minutes, the user must re-enter the password to re-activate the terminal.

All sensitive areas are monitored by 3 (three) cameras.

Customer's general policies:

It is prohibited to register any customer using paper or any type of hand writing notes. All information must be directly inputted into GlobalNova's system;

It is prohibited to provide any customer's information to third parties except to the customer him/herself;

Customers are not required to provide any bank or credit card information for a second time, except when updating with a different bank or credit card information;

It is prohibited to charge customer's bank/credit card without his/her authorization;

It is prohibited to change any customer's information or input any personal information without his/her authorization;

It is prohibited to access GlobalNova's systems using someone else's user/password;

All suspicious accounts are canceled and any charges returned to the customers. GlobalNova acknowledges as fraudulent any transaction made without customer's authorization.